AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions and listings of claims in the application.

Listing of Claims:

Claim 1 (Previously Presented): A method for secure communications between a client and a server, comprising:

managing a communications negotiation between the client and the server through an intermediate device that supports a direct mode and a proxy mode;

receiving encrypted data packets from the client with the intermediate device;

decrypting each encrypted data packet with the intermediate device;

forwarding unencrypted data packets from the intermediate device to the server using a communication session negotiated by the client and the server when the intermediate device operates in direct mode;

forwarding unencrypted data packets from the intermediate device to the server using a communication session negotiated by the server and the intermediate device when the intermediate device operates in proxy mode;

receiving data packets from the server;

encrypting the data packets from the server; and

forwarding encrypted data packets to the client.

Claim 2 (Previously Presented): The method of claim 1 wherein said step of managing comprises:

receiving TCP session negotiation data from the client and modifying the negotiation data prior to forwarding the negotiation data to the server to establish the communications session between the client and the server when operating in direct mode.

Claim 3 (Original): The method of claim 2 wherein the method includes the further step of modifying a SYN request from the client to the server to alter the packet transmission parameters.

Claim 4 (Original): The method of claim 3 wherein said step of modifying includes modifying at least a maximum segment size value of said data packet.

Claim 5 (Previously Presented): The method of claim 1, wherein the method further includes the steps of negotiating an SSL session with the client.

Claim 6 (Previously Presented): The method of claim 1 wherein decrypting comprises decrypting SSL encrypted packet data, and wherein encrypting comprises encrypting a data packet with SSL.

Claim 7 (Previously Presented): The method of claim 1 wherein said step of managing comprises receiving with the intermediate device communication negotiation data directed to the server from the client and responding to said negotiation in place of the server when the intermediate device operates in proxy mode.

Claim 8 (Previously Presented): The method of claim 7 further including negotiating the communications session between the server and the intermediate device as a separate TCP session.

Claims 9-10 (Cancelled).

Claim 11 (Previously Presented): The method of claim 1 further including the step, prior to said step of receiving encrypted data, of negotiating an encrypted data communications session between the intermediate device and the client.

Claim 12 (Original): The method of claim 1 wherein said step of managing comprises maintaining a database of entries on each session of data packets communicated between the client and the server.

Claim 13 (Original): The method of claim 12 wherein said database includes an entry for a session comprising a session ID, a TCP Sequence number and an SSL session number.

Claim 14 (Original): The method of claim 12 wherein said entry further includes an initialization vector.

Claim 15 (Original): The method of claim 12 wherein said entry includes an expected ACK.

Claim 16 (Original): The method of claim1 wherein said step of receiving encrypted data packets includes receiving data packets including encrypted application data spanning multiple packets, and said step of forwarding includes forwarding a portion of the application data contained in an individual encrypted TCP segments to the server without authentication.

Claim 17 (Original): The method of claim 16 further including the step of authenticating the application data on receipt of all packets including the application data.

Claim 18 (Original): The method of claim 16 wherein said data is not buffered during decryption.

Claim 19 (Original): The method of claim 16 wherein said data is buffered for a length sufficient to complete a block cipher used to encrypt the data.

Claim 20 (Previously Presented): A method for secure communications between a client and one of a plurality of servers performed on an intermediary device, comprising:

establishing a communications session between the client and said one of said plurality of servers by receiving negotiation data from the client intended for the server and forwarding the negotiation data in modified form to the server, and receiving negotiation data from the server intended for the client and forwarding the negotiation data to the client to establish the client and the server as terminations for the communications session;

establishing a secure communications session between the client and the intermediary device;

maintaining a database of the secure communications session including information on the session/packet associations;

receiving encrypted application data from the client at the intermediary device by the secure communications session between the intermediary device and the client;

decrypting the application data; and

forwarding decrypted application data from the intermediary device to said one of said plurality of servers using the communications session established between the client and the server.

Claim 21 (Previously Presented): The method of claim 20 further including the steps of:

receiving at the intermediary device application data from the server destined for the client;

encrypting the application data at the intermediary device; and

forwarding the application data to the client along the secure communication session established between the intermediary device and the client.

Claim 22 (Original): The method of claim 20 wherein the method further includes the step of selecting one of the plurality of servers for each packet in the communications session and mapping all communications intended for the server to said one of said plurality of servers.

Claim 23 (Previously Presented): The method of claim 21 wherein forwarding the application to the data comprises receiving packets from said one of said plurality of servers and modifying the source and destination addresses of the packet to forward the packet to the client.

Claim 24 (Currently Amended): The method of claim 20, wherein said step of decrypting application data comprises decrypting data and forwarding said data on to said one of said plurality of servers via a secure network.

Claim 25 (Original): The method of claim 24 further including the step of receiving application data from said one of said plurality of servers, encrypting said data, and forwarding encrypted data to said client.

Claim 26 (Original): The method of claim 20 wherein said database includes an entry for a session comprising a session ID, a TCP Sequence number and an SSL session number.

Claim 27 (Original): The method of claim 20 wherein said entry further includes an initialization vector.

Claim 28 (Original): The method of claim 20 wherein said entry includes an expected ACK.

Claim 29 (Original): The method of claim 20 wherein said step of forwarding includes:

forwarding data which spans over multiple TCP segments and forwarding data which is not authenticated.

Claim 30 (Original): The method of claim 29 wherein said data is not buffered during decryption.

Claim 31 (Original): The method of claim 29 wherein said data is buffered for a length sufficient to complete a block cipher used to encrypt the data.

Claim 32 (Original): The method of claim 29 wherein said step of forwarding includes authenticating the decrypted data after a final segment of a multi-segment encrypted data stream is received.

Claim 33 (Previously Presented): An acceleration apparatus coupled to a public network and a secure network, communicating with a client via the public network and communicating with one of a plurality of servers via the secure network, comprising:

a network communications interface;

at least one processor;

programmable dynamic memory;

a communications channel coupling the processor, memory and network communications interface;

a client/server open communications session manager;

a client secure communication session manager;

a client/server secure communications session tracking database;

and

a data packet encryption and decryption engine,

wherein the acceleration apparatus is adapted to operate in a direct mode and a proxy mode,

wherein in the direct mode the acceleration apparatus decrypts data packets received from the client and forwards the decrypted data packets to one of the servers using a communication session negotiated by the client and the server,

wherein in the proxy mode the acceleration apparatus responds to the client on behalf of the server and forwards the decrypted data packets to the server using a communication session negotiated by the acceleration device and the server.

Claim 34 (Previously Presented): The apparatus of claim 33 wherein in the proxy mode the client open communications session manager and secure communication manager enable the apparatus as a TCP and SSL proxy for the server.

Claim 35 (Previously Presented): The apparatus of claim 33 wherein in the direct mode the communications session manager enables transparent secure and open communication between the client and the server.

Claim 36 (Cancelled).

Claim 37 (Previously Presented): The apparatus of claim 33 further including a load selection manager balancing the routing of multiple open and secure communications session between a plurality of clients and a plurality of servers based on current processing levels of the servers.

Claim 38 (Original): The apparatus of claim 33 wherein data packet encryption and decryption engine performs SSL encryption and decryption on data packets transmitted between the client and said at least one server.

Claim 39 (Original): The apparatus of claim 41 wherein the session tracking set maintains database having at least one record per communication session between the client and server.

Claim 40 (Original): The apparatus of claim 33 wherein said session tracking database includes a TCP sequence number and an SSL sequence number.

Claim 41 (Previously Presented): The apparatus of claim 33 further including a recovery manager coupled to the database.

Claim 42 (Original): The apparatus of claim 33 wherein said data is not buffered during decryption.

Claim 43 (Original): The apparatus of claim 33 wherein said data is buffered for a length sufficient to complete a block cipher used to encrypt the data.

Claim 44 (Previously Presented): The apparatus of claim 33 wherein said client/server open communications session manager performs an authentication process that discards at least a portion of the decrypted, unauthenticated packet application data from the client prior to receiving a final segment of the application data and authenticates the decrypted data using only the remaining portion of the application data.

Claim 45 (Currently Amended): A secure sockets layer processing acceleration device, comprising:

a communication engine establishing a secure communications session with a client device via an open network;

a server communication engine establishing an open communications session with a server via a secure network; and

an encryption and decryption engine operable on encrypted data packets received via the open communications session and on clear data received via the open communications session,

wherein the communication engine supports: (1) a direct mode in which decrypted data packets are ~~is~~ forwarded to the servers using a communication session negotiated by the client and the server, and (2) a proxy mode in which the acceleration device responds to the client on behalf of the server and forwards the decrypted data packets to the server using the open communications session established by the acceleration device and the server.

Claim 46 (Previously Presented): The SSL acceleration device of claim 45 wherein when operating in direct mode the communication engine forwards modified communication session data to the server over the communication session between the client device and the server.

Claim 47 (Currently Amended): The SSL acceleration device of claim 45 wherein when operating in ~~the~~ proxy mode the communication engine acts as a proxy for a plurality of servers in communication with the SSL acceleration device.

Claim 48 (Original): The SSL acceleration device of claim 45 further including a session tracking database interacting with the encryption and decryption engine tracking client and server communications.

Claim 49 (Original): The SSL acceleration device of claim 45 wherein the encryption and decryption engine includes a bufferless mode transmitting decrypted, unauthenticated data to a server.

Claim 50 (Previously Presented): The SSL acceleration device of claim 45 further including a load balancing engine that selects the server from a plurality of servers based on a load balancing algorithm that calculates current processing loads associated with each of the servers.

Claim 51 (Previously Presented): The method of claim 1, further comprising automatically switching the intermediate device from the direct mode to the proxy mode upon detecting a communication error associated with the direct mode.

Claim 52 (Previously Presented): The apparatus of claim 33, wherein the acceleration apparatus automatically switches from the direct mode to the proxy mode upon detection of a communication error associated with the communication session negotiated by the client and the server.

Claim 53 (Currently Amended): The SSL acceleration device of claim 45, wherein the communications engine automatically switches from the direct mode to the proxy mode upon detection of a communication error with the communication session negotiated by the client and the server.